IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 22, 2018, accepted March 6, 2018, date of publication April 2, 2018, date of current version April 25, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2819424

A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold

FERDA ERNAWAN AND MUHAMMAD NOMANI KABIR
Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Gambang 26300, Malaysia
Corresponding author: Ferda Ernawan (ferda1902@gmail.com).

This work was supported by Universiti Malaysia Pahang through the Research Grant Scheme, Ministry of Higher Education, under Grant RDU160102.

ABSTRACT This paper presents a reliable digital watermarking technique that provides high imperceptibility and robustness for copyright protection using an optimal discrete cosine transform (DCT) psychovisual threshold. An embedding process in this watermarking technique utilizes certain frequency regions of DCT, such that insertion of watermark bits causes the least image distortion. Thus, the optimal psychovisual threshold is determined to embed the watermark in the host image for the best image quality. During the insertion of watermark bits into the certain frequencies of the image, watermark bits are not directly inserted into the frequency coefficient; rather, the certain coefficients are modified based on some rules to construct the watermarked image. The embedding frequencies are determined by using modified entropy finding large redundant areas. Furthermore, the watermark is scrambled before embedding to provide an additional security. In order to verify the proposed technique, our technique is tested under several signal processing and geometric attacks. The experimental results show that our technique achieves higher invisibility and robustness than the existing schemes. The watermark extraction produces high image quality after different types of attacks.

INDEX TERMS Image watermarking, modified entropy, embedding scheme, extraction scheme, psychovisual threshold.

I. INTRODUCTION

With the rapid growth of internet technology, illegal copy, transmission and distribution of digital multimedia become an important security issue. This issue motivates for developing a solution for image authentication and copyright protection. Digital watermarking considered as an alternative solution to prevent illegal copy has drawn widespread attention [1]. The watermark insertion and extraction may be done by the owner to ensure and verify its ownership and authenticity by using digital watermarking process. In general, watermarking can be done either in spatial domain in which watermarks are embedded in the image pixels directly or in frequency domain where the watermark is inserted in the frequencies obtained by frequency transformation of the image [2]. Robustness in the spatial domain is a major issue as it is easy to identify the watermark inserted in the spatial domain [3]. Watermarking techniques based on frequency domains with the transformations such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Integer Discrete Wavelet Transform (IDWT) have been used in last decade due to high robustness and imperceptibility. However, DWT and IDWT require a large computational complexity.

A reliable digital watermarking technique needs to satisfy certain properties [4], [5] such as imperceptibility, robustness, undetectable, security and blind extraction. The embedded watermark into the host image should produce less distortion such that the watermark effect cannot be detected by the human visual system. The watermarking techniques should ensure the quality closer to the original host images. Watermarks must withstand the common signal processing and geometrical attacks e.g., filtering, noise addition, image compression, size change, cropping and change of pixel values. Due to the limited size of the watermark that can be embedded into a host image, a binary watermark is the best choice. The purpose of a watermarking technique is to secure the watermark inside the image such that the watermark is extremely difficult to be found and destroyed by attackers. A blind watermarking technique provides an independent watermark recovery without referring to the original host image. It is challenging to develop a blind watermarking technique that is robust and imperceptible

with a good security property and less computational complexity.

II. RELATED WORK

To enhance the robustness and imperceptibility of the watermarked images, researchers nowadays work on the hybrid watermarking techniques based on frequency and matrix decomposition [6]–[8]. In the watermarking scheme proposed in [9] and [10], a watermark is embedded into the frequency coefficients with scaling factors. This scheme provides a good level of robustness to the recovered watermark under different types of attacks; however, the imperceptibility of the watermarked image needs to be improved.

Many research works have been conducted on image watermarking techniques. In 2011, Lai's scheme [7] presented a novel watermarking method based on the human visual system with singular value decomposition (SVD) of DCT matrix B of the image, i.e., $B = U^T DV$ where U and V are the orthogonal matrices and D is a diagonal matrix. A binary watermark image is embedded into the host image by modifying U orthogonal matrix. Specifically, the watermark bits are inserted by modifying $U_{3,1}$ and $U_{4,1}$ coefficients from the hybrid DCT-SVD. This scheme reportedly provides better performance in terms of robustness under noise addition, histogram equalization, scale and Gaussian low-pass filter. While the watermark embedding capacity is still insufficient, the robustness of watermarked image needs to be enhanced.

Roy and Pal [11] proposed a watermarking scheme that embeds multiple watermark bits in the middle band coefficients following a zig-zag order. This method can produce better robustness under noise addition, JPEG compression, and sharpening. This scheme performs sequential embedding process from left-corner to the right, from top to bottom. The diversity of embedded block regions needs to be improved, such that the watermark image is difficult to be recovered. In this scheme, 22 coefficients are modified in the middle frequency band of DCT. This scheme provides a large embedding capacity which is about 11 bits for each block, which results in significant distortion in quality of the watermarked image.

Das *et al.* [12] presented a blind watermarking based on the inter-block coefficient correlation. This scheme embeds a watermark image according to the different adjacent blocks. This technique provides better robustness under JPEG compression than the other techniques. However, the robustness of the watermarked image against noise addition, Gaussian filter and sharpening needs to be improved.

Singh and Singh [13] proposed a watermarking technique where the watermark image is split into two parts – one with the most significant bits and the other with the least significant bits. Then the watermark is embedded by modifying the singular values of DWT-SVD. The watermark cannot be perfectly extracted even under no attack. Furthermore, the technique provides weak robustness under histogram equalization.

Islam and Laskar [14] presented a watermarking scheme based on lifting wavelet transform (LWT) and singular value decomposition (SVD). The selected third-level LWT of the sub-band HL3 is divided into 2×2 non-overlapping blocks for embedding the watermark bits. This scheme has a limited watermark capacity of 1024 bits. Furthermore, there is no option to select embedding locations due to the limited capacity. Their scheme produces the average PSNR values of 43 dB.

A watermark logo with a binary image is able to produce less distortion in the watermarked image than a grayscale watermark or a color watermark. A color watermark has been used in several watermarking schemes [15]. A color watermark provides larger information capacity that significantly affects the imperceptibility of the watermarked image. Therefore, a minimum number of bits in a binary watermark is important to produce a higher invisibility of the watermarked images. Many watermarking schemes have introduced the binary watermark logo as copyright information [16]. A scrambled binary watermark provides extra security for image watermarking. It ensures that only the owners or authorized body can extract the watermark from the host image. It is challenging to develop a watermarking scheme that provides an improved robustness and quality of the watermarked images with less distortion and extra security.

This paper presents a new embedding technique by examining certain DCT coefficients in the middle frequency based on a psychovisual threshold. Embedding regions are determined based on the lowest modified entropy value of the image blocks. The lowest modified entropy value indicates the highest redundant image information. Binary watermark bits are scrambled before they are embedded into the selected coefficients. The proposed technique has been tested under different types of attacks. Test results have been verified with other schemes in terms of *Normalized cross-Correlation* (NC) and *Structural SIMilarity* (SSIM) index. This paper is organized as follows. Modified entropy for representing visual characteristics is described in Section II. The watermark embedding and extraction algorithms are presented in Section III. Experimental results are provided in Section IV. Finally, the conclusion is given in Section V.

III. HUMAN VISUAL CHARACTERISTICS

Visual entropy and edge entropy considering human visual characteristics provide the most significant part of the host image to embed a watermark [7]. Thus, visual entropy and edge entropy can be used to select the region of embedding blocks. Entropy values indicate less distortion areas that are suitable for watermark embedding as these areas do not have significant distortion effect in the host image. Combination entropy and edge entropy can be used to select the significant embedding watermark. The modified entropy of an N-state is defined by:

$$E_p = -\sum_{i=1}^{N} \frac{p_i \exp(1 - p_i) + p_i \log_2(p_i)}{2} \quad (1)$$

where p_i denotes the occurrence probability of i-th pixel with $0 \leq p_i \leq 1$ and $1 - p_i$ represents the uncertainty or ignorance of the pixel value.

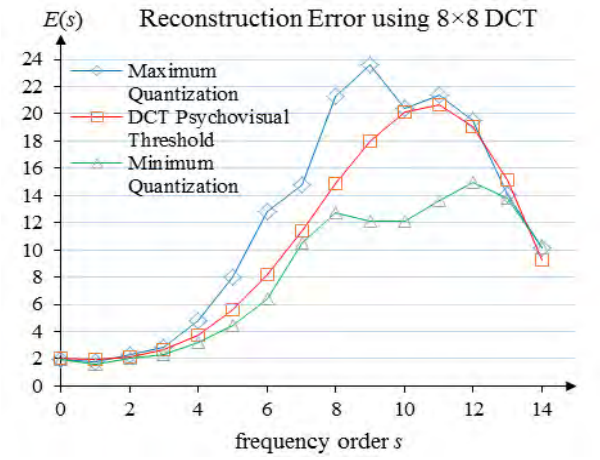

FIGURE 1. DCT psychovisual threshold.

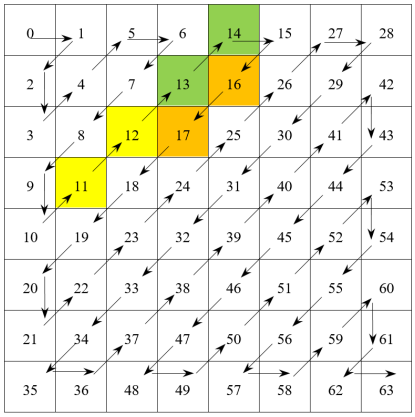

FIGURE 2. Selected DCT coefficient pairs based on the psychovisual threshold.

IV. PSYCHOVISUAL THRESHOLD

Referring to the psychovisual threshold [17]–[27], the gaps between the psychovisual threshold and minimum quantization values of JPEG compression can be utilized to embed the watermarks. These gaps can be noticed between the curve marked with squares and the curve marked with triangles as shown in Figure 1 which plots the reconstruction errors E of DCT psychovisual threshold, maximum quantization and minimum quantization values, over the frequency order s. The DCT coefficients are arranged in a zig-zag order as shown in Figure 2. Considering the gap between the psychovisual threshold (the curve marked with squares) and the minimum quantization value (the curve marked with triangles) in the frequency order between 4 and 5, some coefficients are selected for watermark embedding. These gaps can be measured as follows:

$$Q_G = Q_{psy} - Q_{\min} \tag{2}$$

where Q_G denotes the gap between the reconstruction errors, Q_{psy} and Q_{min} in which Q_{psy} represents the error with DCT psychovisual threshold and Q_{min} indicates the error with the minimum quantization. The DCT coefficients are selected in the lower frequencies. The selected coefficients are ordered into a vector of coefficients as shown in Figure 3. We assume that those locations provide less distortion and more robustness under image compression attacks.

FIGURE 3. Selected coefficient pairs for embedding watermark.

This experiment uses two thresholds: α and β, where α denotes a threshold for the first coefficient and β represents a threshold for the second coefficient. The thresholds α and β are set as negative or positive values based on the certain condition as given in Algorithm 1.

Algorithm 1 Setup of Threshold Values

```
Input: T, A
Output: α, β
for x = 0 to 2
    if (A(2x) < 0) then
        α = −T;
    else
        α = T;
    end (if)
    if (A(2x+1) < 0) then
        β = −T;
    else
        β = T;
    end (if)
end (for)
```

In the algorithm, T represents a threshold value obtained from the trade-off between the imperceptibility and robustness of the watermarked image under JPEG compression. T is measured based on the relationship between SSIM and NC values. Based on the experimental results, we find an optimal threshold T for Lai's scheme [7] and our proposed technique as shown in Figures 4 and 5. We find an optimal threshold for U orthogonal matrix from the hybrid DCT-SVD as 0.016; and the middle DCT coefficient as about 20.

A. EMBEDDING ALGORITHMS

Watermark embedding process is described in Figure 6 and Algorithm 2. Referring to Figure 6, a host image is divided into non-overlapping blocks of 8×8 pixels. Embedding blocks are selected based on the modified entropy values. The number of selected blocks is considered to be the same as the number of watermark pixels. In this research, we use a binary watermark with the size 32×32 pixels. Therefore, 1024 of

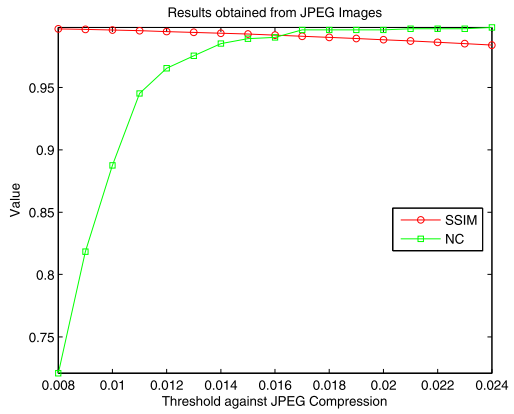

FIGURE 4. Trade-off between SSIM and NC values for Lai's scheme [7].

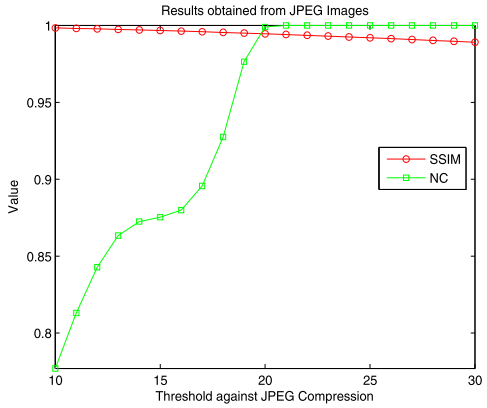

FIGURE 5. Trade-off between SSIM and NC values for the proposed technique.

4096 blocks are selected to embed the watermark logo. In the algorithm 2, watermarks are embedded in the frequency coefficients of each selected block of an image using the technique given in step 8. Note that for $x = 0$, 1, and 2, $A(2x)$ represents A (0), $A(2)$, A (4) and $A(2x + 1)$ denotes A (1), $A(3)$, $A(5)$, respectively as shown in Figure 3. α and β present variant thresholds for watermark embedding. If $A(y) < 0$, for $y = 0, 1, \ldots, 5$, the threshold value is negative; otherwise, the threshold is positive as given in Algorithm 1.

The locations of watermark embedding are stored to determine the selected blocks during watermark extraction. Selected blocks based on modified entropy are chosen which has large redundant data. Attackers may identify the selected block, while they will find it difficult to identify the scrambled watermark.

B. EXTRACTION ALGORITHMS

Watermark extraction process is described in Figure 7 and Algorithm 3.

V. EXPERIMENTAL RESULTS

In this experiment, a binary logo image with 32×32 pixels is used as a watermark. The logo is scrambled by Arnold

Algorithm 2 Embedding Watermark

Input: Host image; watermark; threshold (α and β)

Pre-processing:

Step 1: The cover image of size $M \times N$ is divided into 8×8 non-overlapping blocks.

Step 2: Modified entropy for each non-overlapping block is computed by Equation (1).

Step 3: Blocks that have lowest modified entropy values are selected and their x and y coordinates are saved.

Step 4: The binary watermark is scrambled using Arnold chaotic map

Step 5: Selected blocks are converted into frequencies using DCT.

Step 6: DCT coefficients are converted into a vector by using zig-zag order as shown in Figure 2.

Step 7: Certain coefficients based on the psychovisual threshold as shown in Figure 3 are selected.
bf Watermark embedding:

Step 8: Each bit of binary watermark is embedded according to the rules as follows:

```
U = 1;
for x = 0 to 2
    if U <= length(Watermark) then
        if Watermark(U) = 1 then
            if (|A(2x)| < |A(2x+1)|) then
                C = A(2x);
                A(2x) = A(2x+1)+β;
                A(2x+1) = C;
            else
                A(2x) = A(2x)+α;
                A(2x+1) = A(2x+1);
            end (if)
        else
            if (|A(2x)| < |A(2x+1)|) then
                A(2x) = A(2x)+β;
                A(2x+1) = A(2x+1);
            else
                C = A(2x);
                A(2x) = A(2x+1);
                A(2x+1) =C+α;
            end (if)
        end (if)
        U = U+1;
    end (if)
end (for)
```

for $x = 0$, 1, and 2, $A(2x)$ represents $A(0)$, $A(2)$ and $A(4)$ and $A(2x + 1)$ denotes $A(1)$, $A(3)$ and $A(5)$. α and β present variant threshold for watermark embedding. If $A(2x) < 0$ or $A(2x + 1) < 0$, the threshold value is negative, otherwise the threshold is positive.

Post-processing:

Step 9: The modified values of the vector are set into the two-dimensional matrix in Figure 2.

Step 10: The inverse DCT on each selected block is performed.

Step 11: The modified selected blocks are merged to reconstruct the watermarked image.

Output: Watermarked image containing a logo

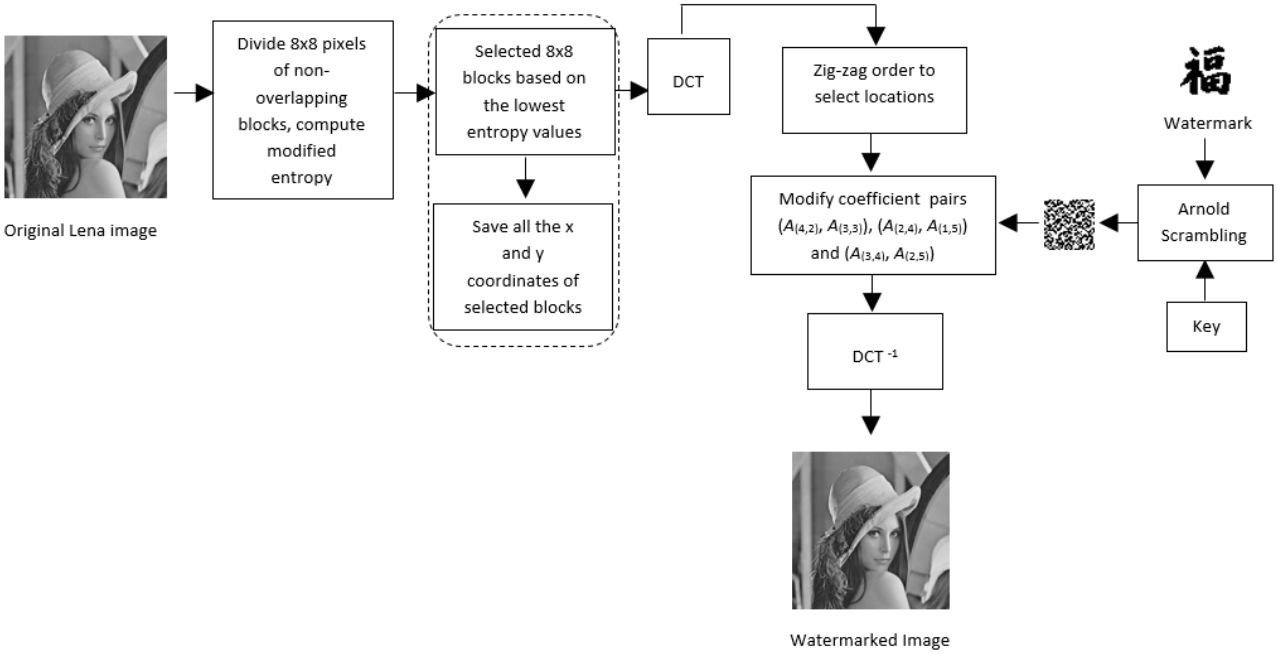

FIGURE 6. Schematic block diagram of the proposed technique for watermark insertion.

Algorithm 3 Watermark Extraction

Input: Watermarked image; locations (x and y coordinates) of the selected blocks; Threshold (α and β)

Pre-processing:

Step 1: x and y coordinates stored during watermark insertion are used to extract the watermark. Each selected block is transformed using DCT.

Step 2: Each DCT block-based is converted into a vector using zig-zag order.

Watermark extraction:

Step 3: Certain coefficients as shown in Figure 3 are selected. Each watermark bit is recovered according to the following rule as follows:
if $A_k < A_{k+1}$ for k = 0,2,4 **then**
watermark bit =1,
else
watermark bit =0.
end (**if**)

Post-processing after embedding:

Step 4: The scrambled binary watermark is inversed by Arnold chaotic map to obtain the original watermark.

Output: Watermark recovery

chaotic map to provide additional security as demonstrated in Figure 8. Our technique has been investigated with nine grayscale images [28] of size 512×512 pixels as shown in Figure 9.

The proposed technique is tested under different types of attacks such as average filter, Wiener filter, median filter, Gaussian low pass, Gaussian noise, speckle noise, pepper and salt noise, sharpening, Poisson noise, adjust, histogram equalization attack, cropping, scaling, jpeg compression and combination attacks. The performance of our technique is evaluated by imperceptibility and robustness. Imperceptibility is measured by Absolute Reconstruction Error (ARE) defined by:

$$ARE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}|g(i,j) - f(i,j)| \tag{3}$$

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(g(i,j) - f(i,j))^2} \tag{4}$$

where $g(i,j)$ denotes the pixel value of the original image and $f(i,j)$ implies the pixel value of the compressed image. The imperceptibility of the proposed technique is measured by Structural SIMilarity (SSIM) index defined as:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma} \tag{5}$$

where $\alpha > 0$, $\beta > 0$, $\gamma > 0$, are parameters which can be adjusted to signify their relative importance. Robustness of our technique has been evaluated by Normalized Cross-Correlation (NC) and Bit Error Rate (BER) after applying different types of attacks. NC and BER are

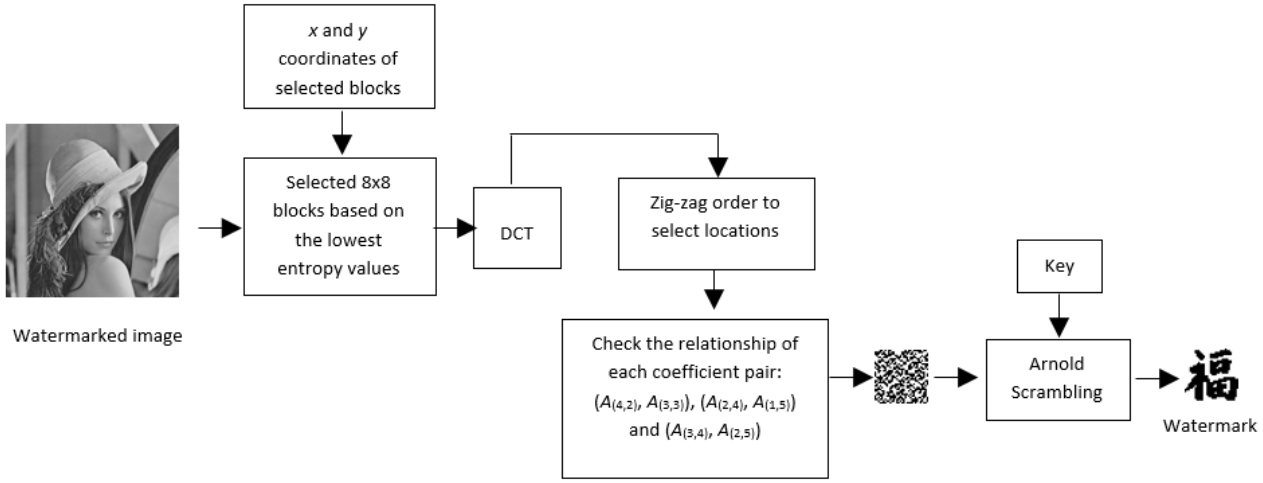

FIGURE 7. Schematic block diagram of the proposed technique for watermark extraction.

FIGURE 8. (a) Binary watermark, (b) Scrambled watermark.

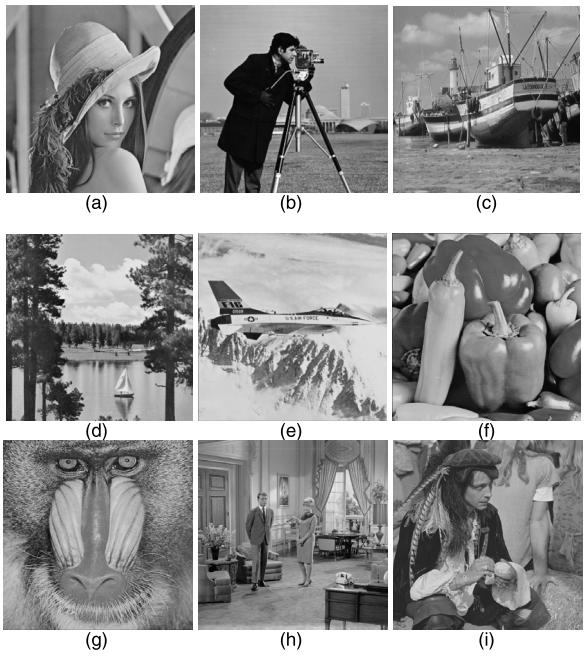

FIGURE 9. (a) Lena, (b) Cameraman, (c) Boat, (d) Sailboat, (e) Airplane, (f) Pepper (g) Baboon, (h) Livingroom, (i) Man images.

defined as

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j).W^*(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2 \sum_{i=1}^{M}\sum_{j=1}^{N} W^*(i,j)^2}} \quad (6)$$

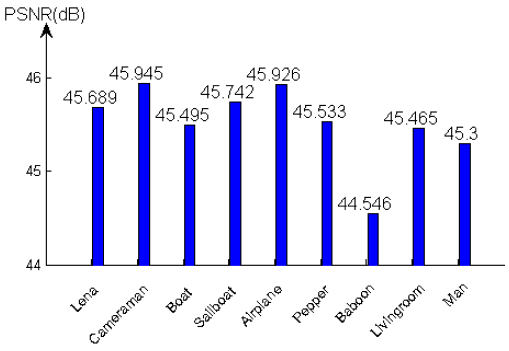

FIGURE 10. The imperceptibility for different images.

TABLE 1. Watermarked image quality.

Image	Lai [7]		Our Scheme	
	ARE	SSIM	ARE	SSIM
Lena	0.375	0.991	**0.312**	**0.994**
Cameraman	**0.272**	0.993	0.303	**0.994**
Boat	0.414	0.992	**0.318**	**0.995**
Sailboat	0.515	0.986	**0.310**	**0.994**
Airplane	0.645	0.983	**0.303**	**0.993**
Pepper	0.369	0.992	**0.317**	**0.994**
Baboon	0.847	0.988	**0.351**	**0.995**
Livingroom	0.454	0.991	**0.319**	**0.996**
Man	0.413	0.992	**0.321**	**0.995**
Average	0.478	0.989	**0.317**	**0.994**

$$BER = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j) \oplus W^*(i,j)}{M \times N} \quad (7)$$

where $W^*(i,j)$ is the extracted watermark and the $W(i,j)$ is the original watermark. M and N denote the row and column sizes. A trade-off between imperceptibility (SSIM) and robustness (NC) is used to determine the threshold value. The experimental results of our scheme are given in Table 1.

Referring to Table 1, our scheme has been verified by ARE and SSIM values that demonstrate less distortion and higher imperceptibility of the watermarked images. The PSNR values of the proposed scheme for different images are presented in Figure 10. Simulation results show that our proposed technique outperforms other existing schemes e.g., Lai's scheme [7].

Our technique is tested under different types of signal processing attacks and compared to other existing schemes. The results of NC values of the extracted watermarks under image processing attacks are depicted in Figure 11. The experimental results show that our technique possesses strong resistance to noise addition and filtering process.

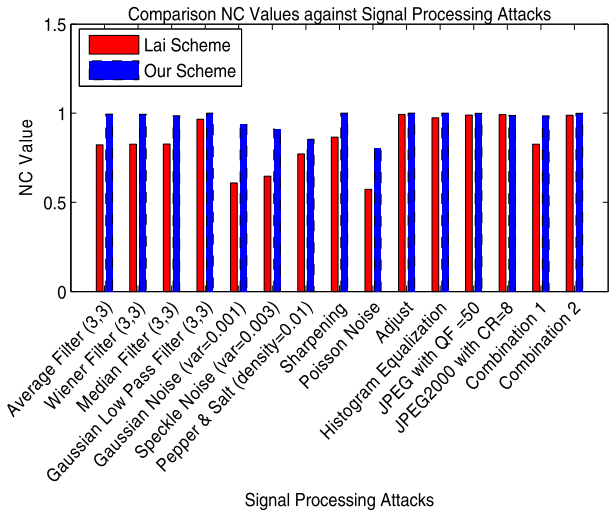

FIGURE 11. Comparison of NC values between Lai's scheme and the proposed technique under image processing attacks.

TABLE 2. Comparison of NC values among the proposed scheme and existing schemes [7], [11], [12] under different types of attack for watermarked Lena image.

Attack	Our scheme	Lai [7]	Roy [11]	Das [12]
JPEG (QF=50)	0.9990	0.9902	**1**	0.9810
JPEG (QF=70)	**1**	1	1	0.9918
Combinational Attacks Pepper & Salt density=0.003) and Median Filter (3,3)	**0.9563**	0.8227	0.8746	0.8641
Salt & Pepper noise, density = 0.01	0.8314	0.7745	**0.9466**	0.8122
Gaussian Noise variance=0.001	**0.9393**	0.6348	0.8998	0.8816
Median filtering with filter size 3×3	**0.9854**	0.8272	0.9687	0.9118
Histogram equalization	**1**	0.9747	0.9313	0.9253

Different NC values of the proposed technique and other existing schemes are listed in Tables 2 and 3 for comparison. In the table, NC values after simulated JPEG compression, median filter, salt & pepper, Gaussian noise and combinational attack between salt & pepper and median filter are presented. We note that Lai's scheme [7] produces a good robustness under image compression. Roy scheme [11] provides better NC value against salt & pepper. However, this scheme does not withstand Gaussian noise attack and histogram equalization. Das scheme [12] provided good NC values under different types of attacks, but still needs to be improved. The proposed method has an average NC = 1 under histogram equalization and NC = 0.9854 under median filter. The proposed scheme is also compared to the scheme

TABLE 3. Comparison of NC values among the proposed scheme and existing schemes [13], [14] under different types of attack for watermarked Lena image.

Attack	Our scheme	Singh [13]	Islam and Laskar [14]
JPEG (QF=30)	0.7769	0.9290	**0.9454**
JPEG (QF=40)	0.8733	0.9428	**0.9764**
JPEG (QF=50)	**0.9990**	0.9461	0.9882
JPEG (QF=60)	**1**	0.9571	0.9912
JPEG (QF=70)	**1**	0.9685	1
Image Sharpening	**1**	0.8616	1
Histogram Equalization	**1**	0.8472	0.9803

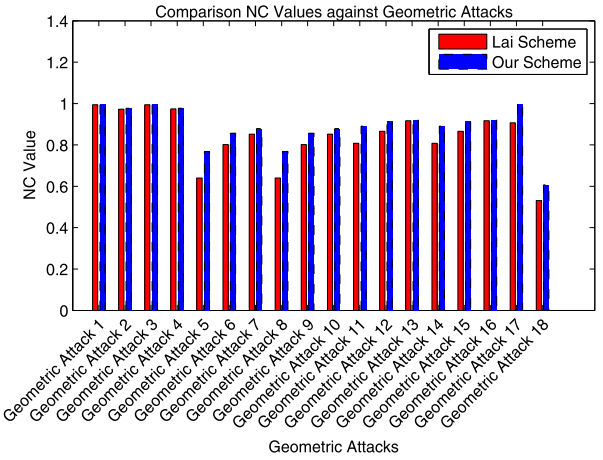

FIGURE 12. Comparison of NC values between Lai's scheme and the proposed technique under geometrical attacks.

TABLE 4. Different types of geometrical attack.

Geometric Attack 1:	Centred Crop 25% (128x128 by black)
Geometric Attack 2:	Centred Crop 50% (256x256 by black)
Geometric Attack 3:	Centred Crop 25% (128x128 by white)
Geometric Attack 4:	Centred Crop 50% (256x256 by white)
Geometric Attack 5:	Crop rows off 50% (256 rows by black)
Geometric Attack 6:	Crop rows off 25% (128 rows by black)
Geometric Attack 7:	Crop rows off 12.5% (64 rows by black)
Geometric Attack 8:	Crop rows off 50% (256 rows by white)
Geometric Attack 9:	Crop rows off 25% (128 rows by white)
Geometric Attack 10:	Crop rows off 12.5% (64 rows by white)
Geometric Attack 11:	Crop columns off (256 columns by black)
Geometric Attack 12:	Crop columns off (128 columns by black)
Geometric Attack 13:	Crop columns off (64 columns by black)
Geometric Attack 14:	Crop columns off (256 columns by white)
Geometric Attack 15:	Crop columns off (128 columns by white)
Geometric Attack 16:	Crop columns off (64 columns by white)
Geometric Attack 17:	Scaling 0.8
Geometric Attack 18:	Scaling 0.25

TABLE 5. Comparison of NC values between Lai's scheme and our scheme under signal processing attacks.

Image Processing attacks	Lena				Cameraman				Airplane			
	Lai's scheme		Our scheme		Lai's scheme		Our scheme		Lai's scheme		Our scheme	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
JPEG with QF =10		**0.4990**	**0.7064**	0.5010		**0.4990**	**0.7064**	0.5010	0.1084	0.4990	**0.7064**	**0**
JPEG with QF =20	0.1438	0.4893	**0.7064**	**0.5010**	0.0255	0.5000	**0.7054**	**0.5020**	0.3221	0.4473	**0.7054**	**0.5020**
JPEG with QF =30	0.7717	0.2021	**0.7769**	**0.2432**	0.6473	0.2900	**0.7254**	**0.2871**	**0.9980**	**0.0020**	0.7583	0.2803
JPEG with QF =40	**0.9642**	**0.0352**	0.8733	0.1553	0.7192	0.2412	**0.8929**	**0.1270**	**0.9980**	**0.0020**	0.8669	0.1650
JPEG with QF =50	0.9902	0.0098	**0.9990**	**0.0010**	0.7004	0.2559	**0.9951**	**0.0049**	**0.9980**	**0.0020**	0.9971	0.0029
JPEG with QF =60	1.0000	0.0000	1.0000	0.0000	0.7040	0.2549	**1.0000**	**0.0000**	1.0000	0.0000	1.0000	0.0000
JPEG with QF =70	1.0000	0.0000	1.0000	0.0000	0.7243	0.2471	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG with QF =80	1.0000	0.0000	1.0000	0.0000	0.7887	0.1973	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG with QF =90	1.0000	0.0000	1.0000	0.0000	0.8720	0.1250	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG2000 with CR=2	1.0000	0.0000	1.0000	0.0000	0.9137	0.0850	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG2000 with CR=4	1.0000	0.0000	1.0000	0.0000	0.9081	0.0908	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG2000 with CR=6	1.0000	0.0000	1.0000	0.0000	0.8707	0.1348	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG2000 with CR=8	0.9913	**0.0088**	0.9882	0.0117	0.8494	0.1641	**1.0000**	**0.0000**	**1.0000**	**0.0000**	0.9922	0.0078
JPEG2000 with CR=10	0.9715	0.0293	**0.9793**	**0.0205**	0.8190	0.1865	**1.0000**	**0.0000**	**0.9990**	**0.0010**	0.9392	0.0605

TABLE 6. Comparison of NC values between Lai's scheme and our scheme under geometrical attacks.

Image Processing attacks	Lena				Cameraman				Airplane			
	Lai's scheme		Our scheme		Lai's scheme		Our scheme		Lai's scheme		Our scheme	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
Rotation (clockwise 5°)	**0.5066**	**0.5166**	0.4942	0.5098	**0.5450**	**0.4922**	0.5015	0.4971	**0.5368**	**0.5020**	0.4936	0.5049
Centred Cropping 25% (128x128 by black)	0.9941	0.0059	**1.0000**	**0.0000**	0.8818	0.1143	**0.9648**	**0.0371**	0.9812	0.0186	**0.9904**	**0.0098**
Centred Cropping 50% (256x256 by black)	0.9723	0.0273	**0.9773**	**0.0234**	0.7544	0.2168	**0.8413**	**0.2061**	0.9205	0.0762	**0.9639**	**0.0381**
Centred Cropping 25% (128x128 by white)	0.9941	0.0059	**1.0000**	**0.0000**	0.8818	0.1143	**0.9648**	**0.0371**	0.9812	0.0186	**0.9904**	**0.0098**
Centred Cropping 50% (256x256 by white)	0.9742	0.0254	**0.9773**	**0.0234**	0.7555	0.2158	**0.8413**	**0.2061**	0.9195	0.0771	**0.9639**	**0.0381**
Cropping rows off 25% (128 rows by black)	0.8014	0.1787	**0.8564**	**0.1807**	0.7800	0.2002	**0.9561**	**0.0469**	0.9238	0.0732	**0.9971**	**0.0029**
Cropping rows off 50% (256 rows by black)	0.6400	0.2949	**0.7680**	**0.3457**	0.5426	0.3574	**0.8593**	**0.1748**	0.7889	0.1885	**0.9352**	**0.0713**
Cropping rows off 25% (128 rows by white)	0.8014	0.1787	**0.8564**	**0.1807**	0.7800	0.2002	**0.9561**	**0.0469**	0.9238	0.0732	**0.9971**	**0.0029**
Cropping rows off 50% (256 rows by white)	0.6400	0.2949	**0.7680**	**0.3457**	0.5426	0.3574	**0.8593**	**0.1748**	0.7889	0.1885	**0.9352**	**0.0713**
Cropping columns off 25% (128 columns by black)	0.8658	0.1250	**0.9168**	**0.0947**	0.7666	0.2090	**0.8485**	**0.1934**	0.8417	0.1455	**0.8839**	**0.1396**
Cropping columns off 50% (256 columns by black)	0.8073	0.1738	**0.8908**	**0.1299**	0.5495	0.3486	**0.7193**	**0.4619**	0.7675	0.2051	**0.8606**	**0.1748**
Cropping columns off 25% (128 columns by white)	0.8658	0.1250	**0.9168**	**0.0947**	0.7666	0.2090	**0.8485**	**0.1934**	0.8417	0.1455	**0.8839**	**0.1396**

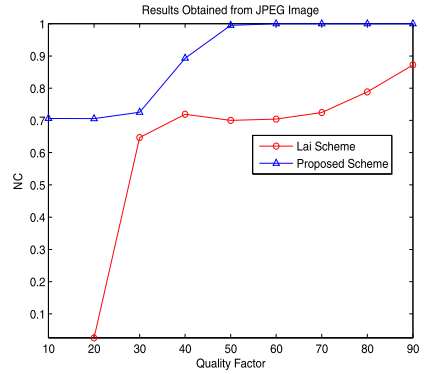

FIGURE 13. Comparison of NC values between Lai's scheme and the proposed technique against JPEG compression.

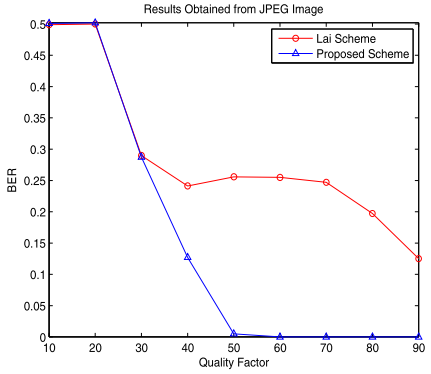

FIGURE 14. Comparison of BER values between Lai's scheme and the proposed technique against JPEG compression.

of Singh and Singh [13], where our scheme provides higher robustness and our scheme achieves NC = 1 under image sharpening. Robustness of the Islam-Laskar scheme is higher when the watermarked image is compressed with a quality factor (QF) less than 50, while our scheme achieves better robustness when the watermarked image is compressed with a QF more than 50.

Overall, the proposed technique is superior to other schemes in terms of imperceptibility and NC values of extracted watermarks.

Experimental results show that our technique outperforms other existing schemes especially under Gaussian noise, median filter and histogram equalization in terms of robustness. It can be checked that our technique produces slightly similar robustness under image compression attacks. The results of the proposed scheme with Lai's scheme under different types of geometrical attacks are presented in Figure 12 for comparison while Table 4 describes the details of the geometrical attacks used for the tests. Our scheme is tested under different types of cropping and scaling attacks. In case of a scaling attack, the watermarked image is scaled by 0.8 and 0.25. In order to extract the watermark, the watermarked image needs to be rescaled or corrected.

TABLE 7. Comparison of NC values between Lai's scheme and our scheme under geometrical attacks.

Image Processing attacks	Lena				Cameraman				Airplane			
	Lai's scheme		Our scheme		Lai's scheme		Our scheme		Lai's scheme		Our scheme	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
Cropping columns off 50% (256 columns by white)	0.8073	0.1738	**0.8908**	**0.1299**	0.5495	0.3486	**0.7193**	**0.4619**	0.7675	0.2051	**0.8606**	**0.1748**
Translation attack (5, 5)	0.5239	**0.5059**	0.5197	0.5010	**0.5562**	**0.5146**	0.5178	0.5049	0.5184	0.5137	**0.5201**	**0.5000**
Scaling 0.8	0.9064	0.0986	**1.0000**	**0.0000**	0.8066	0.2090	**1.0000**	**0.0000**	0.8503	0.1660	**1.0000**	**0.0000**
Scaling 0.5	0.8252	**0.2275**	0.7056	0.3242	0.7190	0.3594	**0.7255**	**0.3076**	**0.7821**	**0.3096**	0.7112	0.3223
Combination Pepper & Salt (density=0.003) and Median Filter	0.8227	0.2129	**0.9864**	**0.0137**	0.8035	0.2217	**0.9961**	**0.0039**	0.8312	0.2148	**0.9912**	**0.0088**
Combination JPEG and Centre Cropping	0.9892	0.0107	**0.9990**	**0.0010**	0.6946	0.2598	**0.9613**	**0.0410**	**0.9892**	**0.0107**	0.9875	0.0127

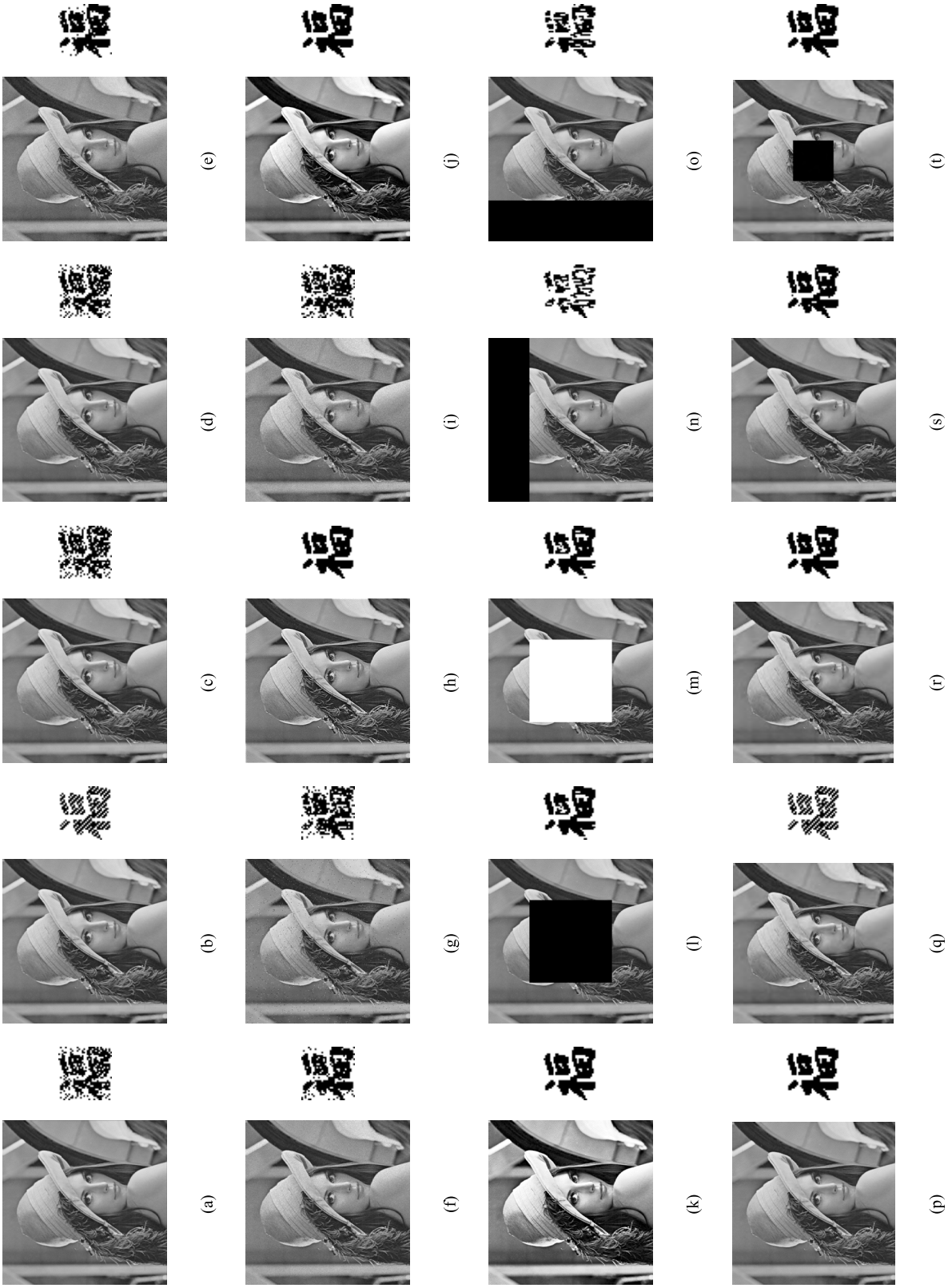

FIGURE 15. Result under different types of attacks and recovered watermark from Lena image (a) Average Filter (3,3) (b) Wiener Filter (3,3) (c) Median Filter (3,3) (d) Gaussian Low Pass Filter (3,3) (e) Gaussian Noise (var = 0.001) (f) Speckle Noise (var = 0.003) (g) Pepper and Salt Noise (density = 0.01) (h) Sharpening (i) Poisson Noise (j) Adjust (k) Histogram Equalization Attack (l) Centred Cropping 50% (256×256 by black) (m) Centred Cropping 50% (256×256 by white) (n) Cropping rows off 25% (128 rows by black) (o) Cropping columns off 25% (128 columns by black) (p) Scaling 0.8 (q) JPEG with QF = 40 (r) JPEG with QF = 50 (s) Combination Pepper & Salt (density = 0.003) and Median Filter (3,3) (t) Combination JPEG with QF = 50 and Centre Cropping 25%.

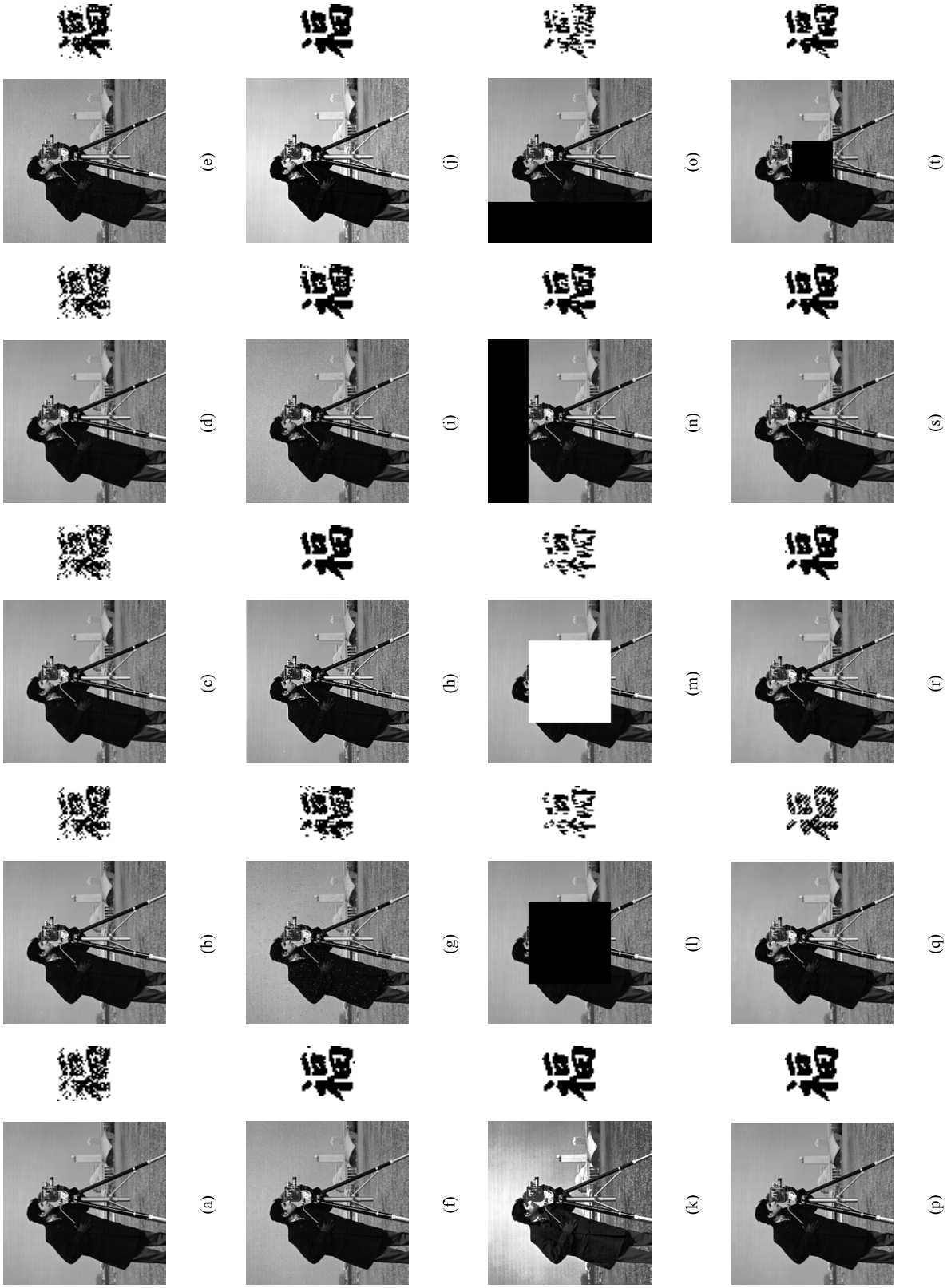

FIGURE 16. Result under different types of attacks and recovered watermark from Cameraman image (a) Average Filter (3,3) (b) Wiener Filter (3,3) (c) Median Filter (3,3) (d) Gaussian Low Pass Filter (3,3) (e) Gaussian Noise (var = 0.001) (f) Speckle Noise (var = 0.003) (g) Pepper and Salt Noise (density = 0.01) (h) Sharpening (i) Poisson Noise (j) Adjust (k) Histogram Equalization Attack (l) Centred Cropping 50% (256×256 by black) (m) Centred Cropping 50% (256×256 by white) (n) Cropping rows off 25% (128 rows by black) (o) Cropping columns off 25% (128 columns by black) (p) Scaling 0.8 (q) JPEG with QF = 40 (r) JPEG with QF = 50 (s) Combination Pepper & Salt (density = 0.003) and Median Filter (3,3) (t) Combination JPEG with QF = 50 and Centre Cropping 25%.

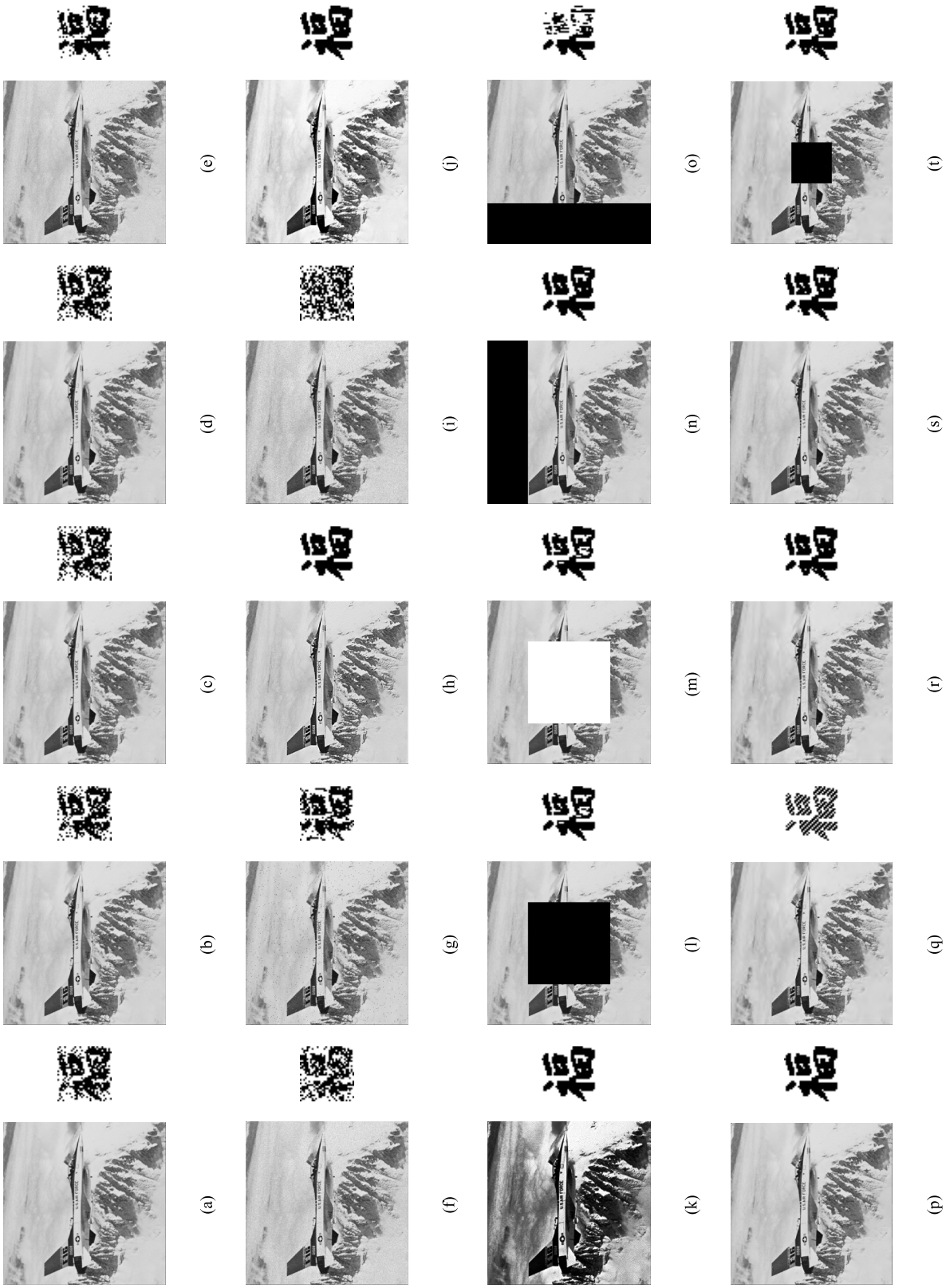

FIGURE 17. Result under different types of attacks and recovered watermark i rom Airplane image (a) Average Filter (3,3) (b) Wiener Filter (3,3) (c) Median Filter (3,3) (d) Gaussian Low Pass Filter (3,3) (e) Gaussian Noise (var = 0.001) (f) Speckle Noise (var = 0.003) (g) Pepper and Salt Noise (density = 0.01) (h) Sharpening (i) Poisson Noise (j) Adjust (k) Histogram Equalization Attack (l) Centred Cropping 50% (256×256 by black) (m) Centred Cropping 50% (256×256 by white) (n) Cropping rows off 25% (128 rows by black) (o) Cropping columns off 25% (128 columns by black) (p) Scaling 0.8 (q) JPEG with QF = 40 (r) JPEG with QF = 50 (s) Combination Pepper & Salt (density = 0.003) and Median Filter (3,3) (t) Combination JPEG with QF = 50 and Centre Cropping 25%.

TABLE 8. Comparison of NC values between Lai's scheme and our scheme under image compression.

Image Processing attacks	Lena				Cameraman				Airplane			
	Lai's scheme		Our scheme		Lai's scheme		Our scheme		Lai's scheme		Our scheme	
	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER	NC	BER
JPEG with $QF=10$		**0.4990**	**0.7064**	0.5010		**0.4990**	**0.7064**	0.5010	0.1084	0.4990	**0.7064**	**0**
JPEG with $QF=20$	0.1438	0.4893	**0.7064**	**0.5010**	0.0255	0.5000	**0.7054**	**0.5020**	0.3221	0.4473	**0.7054**	**0.5020**
JPEG with $QF=30$	0.7717	0.2021	**0.7769**	**0.2432**	0.6473	0.2900	**0.7254**	**0.2871**	**0.9980**	**0.0020**	0.7583	0.2803
JPEG with $QF=40$	**0.9642**	**0.0352**	0.8733	0.1553	0.7192	0.2412	**0.8929**	**0.1270**	**0.9980**	**0.0020**	0.8669	0.1650
JPEG with $QF=50$	0.9902	0.0098	**0.9990**	**0.0010**	0.7004	0.2559	**0.9951**	**0.0049**	**0.9980**	**0.0020**	0.9971	0.0029
JPEG with $QF=60$	1.0000	0.0000	1.0000	0.0000	0.7040	0.2549	**1.0000**	**0.0000**	1.0000	0.0000	1.0000	0.0000
JPEG with $QF=70$	1.0000	0.0000	1.0000	0.0000	0.7243	0.2471	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG with $QF=80$	1.0000	0.0000	1.0000	0.0000	0.7887	0.1973	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG with $QF=90$	1.0000	0.0000	1.0000	0.0000	0.8720	0.1250	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG2000 with $CR=2$	1.0000	0.0000	1.0000	0.0000	0.9137	0.0850	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG2000 with $CR=4$	1.0000	0.0000	1.0000	0.0000	0.9081	0.0908	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG2000 with $CR=6$	1.0000	0.0000	1.0000	0.0000	0.8707	0.1348	1.0000	0.0000	1.0000	0.0000	1.0000	0.0000
JPEG2000 with $CR=8$	0.9913	**0.0088**	0.9882	0.0117	0.8494	0.1641	**1.0000**	**0.0000**	**1.0000**	**0.0000**	0.9922	0.0078
JPEG2000 with $CR=10$	0.9715	0.0293	**0.9793**	**0.0205**	0.8190	0.1865	**1.0000**	**0.0000**	**0.9990**	**0.0010**	0.9392	0.0605

TABLE 9. Comparison of visual perception between Lai's scheme and our scheme under different types of attacks.

Image Processing attacks	Lena		Cameraman		Airplane		Image Processing attacks	Lena		Cameraman		Airplane	
	Lai's scheme	Our scheme	Lai's scheme	Our scheme	Lai's scheme	Our scheme		Lai's scheme	Our scheme	Lai's scheme	Our scheme	Lai's scheme	Our scheme
Average Filter (3,3)							Centred Cropping 25% (black)						
Wiener Filter (3,3)							Centred Cropping 25% (white)						
Median Filter (3,3)							Cropping rows off 25% (black)						
Gaussian Low Pass Filter (3,3)							Cropping rows off 25% (white)						
Gaussian Noise (var=0.001)							Cropping columns off 12.5% (black)						
Speckle Noise (var=0.001)							Cropping columns off 12.5% (white)						
Pepper and Salt Noise (density= 0.003)							Scaling 0.8						
Sharpening							Pepper & Salt (density=0.003) and Median Filter (3,3)						
Histogram Equalization							JPEG and Centre Cropping						

Referring to Figure 12, our technique produces slightly higher NC values than Lai's scheme. Thus, the proposed technique proves that the diagonal frequency order based on the psychovisual threshold can better defend different types of attacks.

The proposed technique proves the supremacy over the existing techniques in terms of adding noise, median filter,

low-pass filter, histogram equalization, cropping and scaling. Furthermore, our scheme produces smaller NC values for image translation and rotation. Our scheme exhibits a weak robustness against rotation and translation of images. Our scheme is also tested under JPEG compression with different quality factors. The robustness of the proposed technique under JPEG compression is displayed in Figure 13. It can be noticed that the proposed technique performs better than the existing Lai's scheme under JPEG compression for different quality factors. With the extreme compression by a quality factor of 10, our technique can produce an NC value of 0.7.

Figure 14 demonstrates the comparison BER values between our technique and Lai's scheme for different quality factors. The figure shows that the proposed technique produces less bit error rate than Lai's scheme under JPEG compression in the range of quality factors between 40 and 90. By using standard image compression with a quality factor of 50, our scheme produces insignificant bit error rate.

Lai's scheme [7] produces good imperceptibility and requires less computation, but does not possess strong robustness property under different attacks. On the other hand, our technique shows better PSNR and SSIM values with smaller error reconstruction and bit error rate. Our scheme also has less computation complexity due to DCT's advantages such as energy compaction properties and it is easy to be implemented. The visual perception of the extracted watermark under different types of image-processing and geometrical attacks is presented in Figures 14, 15 and 16. Our technique has a limitation against Poisson noise, i.e., the visual perception of the extracted watermark can be destroyed by this noise. Moreover, human eye still can recognize the watermark information. The proposed technique performs well under combinatorial attacks such as JPEG compression with image cropping. It reveals that our technique can, not only withstand a single attack, but also subjugate multiple attacks. The visual perception in Figures 14, 15 and 16 demonstrates that the proposed scheme produces a high watermark quality after different types of attacks.

Detailed results of NC and BER values under different types of attacks are listed in Tables 5-8 using the proposed technique and Lai's scheme for three different images – Lena, Cameraman and Airplane. Table 5 presents the results under image processing attacks e.g., noise addition, image filter, median filter, image sharpening, image adjustment and histogram equalization. Tables 6 and 7 provide the results for different types of geometrical attacks. Table 8 lists the results for image compression with JPEG and JPEG2000. Table 9 shows the comparison of visual perception of extracted watermarks between Lai's scheme and our scheme under different types of attacks.

The experimental results show that the proposed technique outperforms Lai's scheme in the aspect of robustness under image processing, geometrical and image compression attacks which can be duly verified by NC and BER values. However, the performance on resisting rotational attacks is not satisfactory. This issue will be further considered in the future work. Overall, it can be stated that our technique is more effective in terms of imperceptibility and robustness than the existing schemes.

VI. CONCLUSION

This paper presents a new embedding technique for image watermarking based on the psychovisual threshold. The watermark bits are embedded by examining the psychovisual threshold on the selected middle-frequency coefficients. A watermark image is not directly embedded into a host image, rather, certain coefficient pairs in the middle frequencies based on the psychovisual threshold are modified with a threshold. Furthermore, a binary watermark is scrambled before it is embedded into the host image to achieve additional security. The human visual characteristics based on the visual entropy and edge entropy are utilized to determine the embedding regions. Furthermore, our scheme is evaluated under different types of attacks such as image noise, low-pass filter, sharpening, median filter, JPEG and JPEG2000, and geometrical attacks like image cropping and scaling. The experimental results demonstrate that our scheme performs better than existing techniques in terms of SSIM and NC values. The proposed technique also provides distorted watermark extraction under image-rotation attack. This issue will be considered in a future research. The proposed scheme also proves the superiority in terms of robustness under multiple combinations of attacks.

REFERENCES

[1] F. Ernawan, M. N. Kabir, M. Fadli, and Z. Mustaffa, "Block-based Tchebichef image watermarking scheme using psychovisual threshold," in *Proc. Int. Conf. Sci. Technol.-Comput. (ICST)*, Oct. 2016, pp. 6–10.

[2] M. Moosazadeha and G. Ekbatanifard, "An improved robust image watermarking method using DCT and YCoCg-R color space," *Optik-Int. J. Light Electron Opt.*, vol. 140, pp. 975–988, Jul. 2017.

[3] S. Kumar, N. Jain, and S. L. Fernandes, "Rough set based effective technique of image watermarking," *J. Comput. Sci.*, vol. 19, pp. 121–137, Mar. 2017.

[4] K. R. Chetan and S. Nirmala, "An efficient and secure robust watermarking scheme for document images using Integer wavelets and block coding of binary watermarks," *J. Inf. Secur. Appl.*, vols. 24–25, pp. 13–24, Oct. 2015.

[5] L.-Y. Hsu and H.-T. Hu, "Blind image watermarking via exploitation of inter-block prediction and visibility threshold in DCT domain," *J. Vis. Commun. Image Represent.*, vol. 32, pp. 130–143, Oct. 2015.

[6] F. Ernawan, M. Ramalingam, A. S. Sadiq, and Z. Mustaffa, "An improved imperceptibility and robustness of 4×4 DCT-SVD image watermarking using modified entropy," *J. Telecommun., Electron. Comput. Eng.*, vol. 9, nos. 2–7, pp. 111–116, 2017.

[7] C. C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," *Opt. Commun.*, vol. 284, no. 4, pp. 938–944, 2011.

[8] X. Wu and W. Sun, "Robust copyright protection scheme for digital images using overlapping DCT and SVD," *Appl. Soft Comput.*, vol. 13, no. 2, pp. 1170–1182, 2013.

[9] N. A. Abu, F. Ernawan, N. Suryana, and S. Sahib, "Image watermarking using psychovisual threshold over the edge," in *Proc. Inf. Commun. Technol.*, vol. 7804. 2013, pp. 519–527.

[10] F. Ernawan, "Robust image watermarking based on psychovisual threshold," *J. ICT Res. Appl.*, vol. 10, no. 3, pp. 228–242, 2016.

[11] S. Roy and A. K. Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks," *AEU Int. J. Electron. Commun.*, vol. 72, pp. 149–161, Feb. 2017.

[12] C. Das, S. Panigrahi, V. K. Sharma, and K. K. Mahapatra, "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation," *Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 244–253, Mar. 2014.
[13] D. Singh and S. K. Singh, "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection," *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13001–13024, 2016.
[14] M. Islam and R. H. Laskar, "Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM," *Multimedia Tools Appl.*, pp. 1–28, 2017.
[15] Q. Su and B. Chen, "A novel blind color image watermarking using upper Hessenberg matrix," *AEU Int. J. Electron. Commun.*, vol. 78, pp. 64–71, Aug. 2017.
[16] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," *Optik-Int. J. Light Electron Opt.*, vol. 127, no. 12, pp. 964–972, 2016.
[17] F. Ernawan, M. N. Kabir, and J. M. Zain, "Bit allocation strategy based on psychovisual threshold in image compression," *Multimedia Tools Appl.*, pp. 1–24, 2017.
[18] F. Ernawan, N. Kabir, and K. Z. Zamli, "An efficient image compression technique using tchebichef bit allocation," *Optik-Int. J. Light Electron Opt.*, vol. 148, pp. 106–119, Nov. 2017.
[19] F. Ernawan, Z. Mustaffa, and L. B. Aji, "An efficient image compression using bit allocation based on psychovisual Threshold," *Int. Inf. Inst. (Tokyo)*, vol. 9, no. 9B, pp. 4177–4182, 2016.
[20] F. Ernawan and S. H. Nugraini, "The optimal quantization matrices for JPEG image compression from psychovisual threshold," *J. Theor. Appl. Inf. Technol.*, vol. 70, no. 3, pp. 566–572, 2014.
[21] F. Ernawan, N. A. Abu, and N. Suryana, "An adaptive JPEG image compression using psychovisual model," *Adv. Sci. Lett.*, vol. 20, no. 1, pp. 26–31, 2014.
[22] N. A. Abu and F. Ernawan, "A novel psychovisual threshold on large DCT for image compression," *Sci. World J.*, vol. 2015, pp. 1–11, Oct. 2015.
[23] N. A. Abu, F. Ernawan, and N. Suryana, "A generic psychovisual error threshold for the quantization table generation on JPEG image compression," in *Proc. 9th Int. Colloq. Signal Process. Appl.*, 2013, pp. 39–43.
[24] F. Ernawan, N. A. Abu, and N. Suryana, "An optimal Tchebichef moment quantization using psychovisual threshold for image compression," *Adv. Sci. Lett.*, vol. 20, no. 1, pp. 70–74, 2014.
[25] F. Ernawan, N. A. Abu, and N. Suryana, "Adaptive Tchebichef moment transform image compression using psychovisual model," *J. Comput. Sci.*, vol. 9, no. 6, pp. 716–725, 2013.
[26] N. A. Abu and F. Ernawan, "Psychovisual threshold on large Tchebichef moment for image compression," *Appl. Math. Sci.*, vol. 8, no. 140, pp. 6951–6961, 2014.
[27] F. Ernawan, N. A. Abu, and N. Suryana, "TMT quantization table generation based on psychovisual threshold for image compression," in *Proc. Int. Conf. Inf. Commun. Technol.*, 2013, pp. 202–207.
[28] R. Rodriguez-Sanchez, J. Martinez-Baena, A. Garrido, J. A. Garcia, J. Fdez-Valdivia, and M. C. Aranda. (2002). *Computer Vision Group*. Univ. Granada, Granada, Spain. [Online]. Available: http://decsai.ugr.es/cvg/dbimagenes/c512.php

FERDA ERNAWAN was born in Semarang, Central Java, Indonesia, in 1988. He received the master's degree in software engineering and intelligence and the Ph.D. degree in image processing from the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka in 2011 and 2014, respectively. He is currently a Senior Lecturer with the Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang. His research interests include image compression, digital watermarking and steganography.

MUHAMMAD NOMANI KABIR received the M.Sc. degree in computational sciences in engineering and the Ph.D. degree in computer science from the University of Braunschweig, Germany. He is currently a Senior Lecturer with the Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, Malaysia. His research interests include issues related to modeling and simulation, computational methods, image processing, and computer networks.